Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 08 July 2004

Daily Overview

- The Arizona Daily Sun reports the fire east of Flagstaff, AZ, has shifted direction, threatening high−voltage power lines that supply electricity to Phoenix and Prescott. (See item 2)

- PC World reports Microsoft's effort last week to fix a vulnerability in the Internet Explorer Web browser and end the latest series of Internet attacks doesn't address another closely related and dangerous vulnerability. (See item 34)

- The Bay City News reports approximately 200 pounds of high explosives have reportedly been stolen from a storage facility in San Mateo, CA, over the holiday weekend. (See item 37)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Web Information

---

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – http://esisac.com]

1. *July 07, Reuters* — **Transocean says jack−up rig damaged. Transocean Inc., the world's largest offshore oil and gas driller, on Wednesday, July 7, said its jack−up rig Trident 20 suffered damage on Saturday, July 3, from a fire in the rig's engine room** while operating off the coast of Turkmenistan in the Caspian Sea. Houston, TX−based Transocean said there were no injuries resulting from the incident and **the cause of the fire is under investigation.** Trident 20's crew has been reduced to just essential personnel. Transocean said the rig, known locally as "the Gurtulush," has been operating under a three−well contract with Malaysia's

Petronas since April 2004. Transocean estimates rig repairs could take two to three months to complete.
Source: http://biz.yahoo.com/rc/040707/energy_transocean_1.html

2. *July 07, Arizona Daily Sun* — **Major power line in fire's path.** Left to burn while monitored by Coconino National Forest fire officers for nearly two weeks, the Jacket fire east of Flagstaff, AZ, shifted direction Monday, July 5, and Tuesday, July 6, threatened high−voltage power lines that supply electricity to Phoenix and Prescott, AZ. The concern with the fire nearing the power lines was not that the flames would take out the lines, but that the dense smoke would act as a conductor and cause the high−voltage lines to arc. **Arizona Public Service reported that if the lines were lost to the wildfire, many of its 700,000 Phoenix area customers could face rolling outages. By Tuesday afternoon, the fire had come within a mile of the 345 kilovolt line that runs from Page, AZ.** The change in direction came as a result of unpredicted easterly winds that blew the fire into the direction of Flagstaff. The winds picked up on Monday. A lightning strike on June 22 started the Jacket fire.
Source: http://www.azdailysun.com/non_sec/nav_includes/story.cfm?sto ryID=90240

3. *July 07, General Accounting Office* — **GAO−04−951T: Energy Markets: Mergers and Many Other Factors Affect U.S. Gasoline Markets (Testimony).** Gasoline is subject to dramatic price swings. **A multitude of factors cause volatility in U.S. gasoline markets, including world crude oil costs, limited refining capacity, and low inventories relative to demand. Since the 1990s, another factor affecting U.S. gasoline markets has been a wave of mergers in the petroleum industry, several of them between large oil companies that had previously competed with each other.** This testimony is based primarily on Energy Markets: Effects of Mergers and Market Concentration in the U.S. Petroleum Industry (GAO−04−96, May 17, 2004). This report examined mergers in the U.S. petroleum industry from the 1990s through 2000, the changes in market concentration (the distribution of market shares among competing firms) and other factors affecting competition in the U.S. petroleum industry, how U.S. gasoline marketing has changed since the 1990s, and **how mergers and market concentration in the U.S. petroleum industry have affected U.S. gasoline prices at the wholesale level.** To address these issues, General Accounting Office (GAO) purchased and analyzed a large body of data and developed state−of−the art econometric models for isolating the effects of eight specific mergers and increased market concentration on wholesale gasoline prices. Highlights: http://www.gao.gov/highlights/d04951thigh.pdf
Source: http://www.gao.gov/new.items/d04951t.pdf

4. *July 07, Reuters* — **EIA sees oil high oil prices for rest of year. Tight global oil supply is likely to keep U.S. crude prices above $35 a barrel for the rest of 2004, U.S. Energy Information Administration (EIA) chief Guy Caruso told Congress on Wednesday, July 7. "While our forecast has crude oil prices easing slightly through third quarter, the world market will still be tight, as world petroleum demand picks up seasonally in the fourth quarter, increasing the potential for unexpected upward price pressure (on oil) this winter,"** Caruso told lawmakers at a House hearing on the petroleum markets. "We continue to expect that the additional crude oil production, which producers with excess capacity have recently committed to provide, would allow for building of crude oil and product inventories," Caruso said. The producers Caruso refers to are those Organization of Petroleum Exporting Countries (OPEC) members with ability to produce more than they have been recently, mainly

Saudi Arabia. Caruso also repeated his warning that, with refineries focusing on making gasoline, the U.S. may enter the upcoming fall and winter season with lower heating oil inventories that could result in higher heating fuel bills for consumers.
Source: http://www.nytimes.com/reuters/business/business−energy−eia− prices.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *July 07, Rocky Mountain Telegram (NC)* — **Tractor−trailer loses chemical containers. State and local fire and law enforcement officials responded to a chemical spill in Edgecombe County, NC,** around midday Tuesday, July 6, a spokesperson for the county central communications office said. Kevin Greene, a telecommunicator for the North Carolina Highway Patrol in Raleigh, said **a tractor−trailer truck lost several containers of Sucker−Plucker −− a chemical used to eliminate unwanted outgrowths on tobacco stalks** −− on NC 42, east of U.S. 258 near Pinetops. "Emergency Management Center and fire department officials were called to clean it up," Greene said. "There was no danger to waterways because of the spill, which was cleared." North Carolina Highway Patrolman Timothy Pope of Troop C investigated the incident, Greene said. The tractor−trailer left the scene. "It is unknown who lost the chemical containers," he said. Volunteers of Pinetops Volunteer Fire Department Station No. 14, the North Carolina Department of Transportation, the Highway Patrol and Edgecombe County Emergency Management Center officials responded to the call.
Source: http://www.rockymounttelegram.com/news/newsfd/auto/feed/news /2004/07/06/1089170793.18121.4071.1078.html;COXnetJSessionID =AsERNtlsKcaT6a1BzUmyMxxzlwi2iDviU4pIJHtsISzPET3HLtpq!185877 1733?urac=n&urvf=10892259370320.7244721017134327

6. *July 07, Global Security Newswire* — **Kyrgyzstan taking steps against chemical attack.** Kyrgyzstan is preparing to respond to possible chemical attacks, the Central Asian nation's public television reported on Tuesday, July 6. **The country's National Security Service mentioned possible terrorist attacks against U.S. citizens deployed at military bases in Kyrgyzstan and neighboring Uzbekistan some days ago. There are 49 waste dumps and 20 chemically dangerous sites in the country, according to the report.** Rescue workers from Kyrgyzstan this week joined their counterparts from Central Asian neighbors Kazakhstan, Tajikistan and Uzbekistan in a five−day chemical and radioactive rescue training session sponsored by the Organization for the Prohibition of Chemical Weapons, according to the Kyrgyz Emergencies Ministry. The training began Monday, July 5, the Associated Press reported.
Source: http://www.nti.org/d_newswire/issues/2004/7/7/001a926c−d881− 49e5−81ff−eb9165488963.html

7. *July 07, Daily American Republic (MO)* — **Several overcome by a chemical mishap. The interaction between two chemicals at NORDYNE Industries sent 12 workers to the hospital Wednesday morning, July 7.** NORDYNE, located in the Poplar Bluff Industrial Park, MO, manufactures heating and cooling products. Poplar Bluff Police and Fire departments, Butler County Emergency Management Agency and Poplar Bluff Regional

Medical Center EMS were called to the scene about 10:45 a.m. after reports that several employees had been exposed to chemical fumes, according to Poplar Bluff Police Detective Gary Pride. **"It is a chemical they use everyday," Pride said. "It just wasn't in the place it was suppose to be." Pride said two different industrial chemicals were being used simultaneously and they produced an unfavorable respiratory irritate that caused workers to have symptoms of lightheadness and nausea, Pride explained.** Within about a half hour a total of 12 employees were transported to the hospital for treatment. Several were overcome by the fumes and at least one reportedly had passed out.
Source: http://www.darnews.com/articles/2004/07/07/news/news1.txt

[Return to top]

Defense Industrial Base Sector

8. *July 07, PostNewsweek Tech Media* — **First phase of JTRS on schedule.** A private contractor and the Army plan to start the early operational assessment phase of the Joint Tactical Radio System (JTRS) by December, the contractor's program manger said Wednesday, July 7. Should the project proceed as planned, the Army could end up buying $20 billion worth of radios over 25 years. Giving a status report on the two−year old JTRS Cluster 1 project, Ralph Moslener, contractor spokesperson, said the company and its partners are on schedule to deliver limited−production radios to the Army, starting next year. He called the Cluster 1 team "trailblazers" who will hand down lessons learned to the other cluster teams. **The JTRS program is one of the foundations of the Department of Defense's evolution toward network−centric operations. The radios will be designed to support multiple waveforms, so joint forces can communicate using a single, upgradeable device.** Because of the size of the JTRS program, it is being rolled out in clusters.
Source: http://www.gcn.com/vol1_no1/daily−updates/26508−1.html

[Return to top]

Banking and Finance Sector

9. *July 07, Bank Technology News* — **A battle's breaking out over phishing prevention.** As phishing and spoofing scams continue to rise on the Web, and identity theft becomes a primary concern for financial services institutions, some credit card issuers have begun experimenting with new card technology to combat the problem. In particular, three card issuers have tested substitute credit card numbers, known as "controlled payment numbers," which let their customers shop online without using their real account numbers. **Experts are divided about the effectiveness of the numbers, but generally agree they provide banks with an added level of protection against at least one kind of identity theft: Internet heists.** At the same time, the numbers are competing against anti−fraud technology introduced in the last couple of years by MasterCard International and Visa U.S.A. A lot is at stake. Identity theft is among the most common security threats that banks and other businesses face today, according to Forrester Research. **According to Forrester, more than half of all identity theft incidents occur in the banking industry, with about 33 percent from credit card fraud alone.**
Source: http://www.banktechnews.com/article.html?id=200407019QJ08C3A

10. *July 06, TechWeb News* — **Corporate losses from Internet−based attacks cost millions. Companies that suffer business disruptions from Internet−based attacks are losing an average of $2 million in revenue, a research firm said Tuesday, July 6. A survey of 162 companies also found that organizations on average suffered one disruptive incident a year from worms, viruses, spyware or other security−related causes, the Aberdeen Group said.** Corporate systems were down an average of 22 hours in each attack. The battle against malicious code has intensified as companies increase their use of the Internet to generate revenue. According to the survey released Tuesday, 75 percent of firms are ratcheting up their Web−based customer sales and services operations, and 55 percent are increasing their use of the Internet for negotiating and buying goods from suppliers. To combat malware, 82 percent of the companies surveyed had strategies focusing on strengthening their defenses. The remaining companies were split, with half saying their primary strategy was to clean up the mess following an attack, or to contain damage once it has occurred. Beyond technology, companies focused on prevention said they needed more staff with strong security backgrounds, the study found.
Source: http://www.techweb.com/wire/story/TWB20040706S0008

11. *July 06, ComputerWorld* — **E−mail glitch exposes private data in California. IT officials in Contra Costa County, CA, on Tuesday, June 6, launched a countywide investigation into how hundreds of internal e−mails containing private employee data were sent out inadvertently to a Swedish company.** The investigation was launched after Computerworld notified the county that Robert Carlesten, a 26−year−old managing director of Internet company Ord&Bild, based in Karlstad, Sweden, could produce dozens of e−mails he said have been arriving at his Internet.ac domain regularly for the past two years. Carlesten said he tried to contact the senders of the e−mails on numerous occasions but received no reply. Many of the e−mails, obtained by Computerworld, contained the names, employee numbers and benefits of Superior Court commissioners and other workers. **A preliminary investigation, said Tom Whittington, CIO of Contra Costa County, revealed that the problem was the result of some county employees using erroneous e−mail address books and wasn't caused by a virus or worm infection.** Part of the problem, said Whittington, is that the county's naming structure includes ".ac" for the auditor controller's office. "Now we need to research who has the bad address book that has this address."
Source: http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,94336,00.html?SKC=home94336

[Return to top]

Transportation Sector

12. *July 07, Transportation Security Administration* — **TSA announces start of Registered Traveler Pilot Program.** The Transportation Security Administration (TSA) on Wednesday, July 7, kicked off the Registered Traveler Pilot Program at the Minneapolis−St. Paul International Airport in Minnesota in conjunction with Northwest Airlines. **Approved registered travelers are now able to use a designated checkpoint lane to provide biometric information (either a finger or iris scan) to confirm identity. Registered travelers and their carry−on bags will still go through primary screening, but more extensive secondary**

screening is largely eliminated. The pilot will expand to four other airports this summer –– Los Angeles International in California in coordination with United Airlines in mid–July; George Bush Intercontinental in Houston, TX, with Continental Airlines in early August; and Boston Logan International in Massachusetss, and Ronald Reagan Washington National in Washington, DC, both with American Airlines by the end of August. The pilot will last about 90 days at each airport. During the pilot, registered travelers can use only the biometric equipment located in the traveler's home airport. Participation in the pilot program is voluntary and free. Once the pilot is complete, TSA will examine the results and technologies for security and customer service benefits.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 00b5e9e

13. *July 07, Associated Press* — **Train travelers stranded in Wisconsin by bomb scare. Authorities investigated a series of bomb threats directed at an Amtrak train Tuesday, July 6, stranding nearly 300 passengers, some of whom had fireworks in their luggage**. The train, running a combined route from Seattle, WA, and Portland, OR, to Chicago, IL, was stopped Tuesday afternoon in Portage, WI, about 80 miles northwest of Milwaukee, WI. The 282 passengers and crew members were taken to a nearby elementary school for questioning while explosive specialists searched the train. Police found that some passengers had fireworks in their luggage, said Columbia County, WI, Sheriff's Lt. Detective Wayne Smith. No other explosives were aboard. The train resumed its trip about 7:30 p.m., more than six hours after it was stopped.
Source: http://hosted.ap.org/dynamic/stories/B/BRF_BOMB_SCARE_TRAIN? SITE=VTRUT&SECTION=HOME&TEMPLATE=DEFAULT

14. *July 07, Mid Hudson News (NY)* — **Stewart International Airport to receive funds for cargo facilities security.** The U.S. Department of Transportation (DOT) announced on Wednesday, July 7, a $200,000 discretionary grant for enhanced cargo area security at Stewart International Airport in New Winsor, NY. **The Federal Aviation Administration (FAA) funding will be used to upgrade the gate security system with remote cameras in the cargo area, said airport Marketing Manager Kiran Jain**. The funding was announced by Senator Charles Schumer on Wednesday. "Safe and secure air service is a critical engine of the Hudson Valley's continued economic growth," he said. "In a post 9/11 era, you can never be too careful." Schumer said the funding will allow Stewart to beef up cargo security to meet today's modern aviation demands.
Source: http://www.midhudsonnews.com/News/SWF–cargo–funds–06Jul04.ht m

15. *July 07, Sun Herald (MS)* — **South Mississippi ports tighten security. South Mississippi ports are complying with new federal guidelines through the installation of radiation monitors to ensure no "dirty bombs" enter the Port of Gulfport inside shipping containers**. In Gulfport, the third busiest container port in the Gulf of Mexico, the monitors will be placed at the east and west terminals. Most of the increased security brought about by the 2002 Maritime Transportation Security Act (MTSA), which went into effect earlier this month, involves more mundane improvements: fencing, lighting, security cameras and personnel. The new measures are designed to protect seaports the same way that airports are protected, in part through checking domestic and foreign commercial vessels as they enter U.S. waters. According to port director, Don Allee, improvements in Gulfport have cost $2.5 million to $3 million, of which the federal government has provided about $2 million.

16. *July 07, Oklahoman* — **Money granted for highway security network.** Nearly two million dollars in new project funding to add to the state's high−tech transportation network was approved Tuesday, July 6, by Oklahoma state transportation commissioners. The money will go toward connecting a series of signs and cameras located on highways throughout the Oklahoma City and Tulsa metro areas. **Transportation officials eventually want 31 sites including homeland security officials, 911 systems, Army National Guard and the state Public Safety Department connected to the system. Known as the Intelligent Transportation System, the program is designed to increase efficiency throughout U.S. highways, according to Alan Stevenson, coordinator of the program for the state Transportation Department**. It allows dispatchers and transportation officials to flash messages to drivers and inspect accident scenes before emergency vehicles arrive. According to Stevenson, the department plans to launch a Website in late 2005, allowing drivers access to the system to check out highways before beginning travel.
Source: http://www.newsok.com/article/1275999/?template=news/main

17. *July 07, PR Newswire* — **Wireless vehicle security and management system to be deployed at Jacksonville seaport.** The Transportation Security Administration (TSA) announced on Wednesday, July 7, that it has awarded a grant to implement a wireless vehicle security and management system at JAXPORT, the Jacksonville, FL, seaport operated by the Jacksonville Port Authority. The new TSA grant is for $1.36 million for Phase I to be completed in 2004. Additional funding can be provided for Phase II system expansion, which would be initiated at the TSA's discretion in fiscal year 2005 for an additional $1.35 million. **The system provides vehicle security, improves fleet manageability, and reduces traffic congestion by incorporating, among other things, wireless GPS vehicle traffic mapping and monitoring and historical capture of vehicles movements for incident investigations.**
Source: http://www.prnewswire.com/cgi−bin/stories.pl?ACCT=SVBIZINK3. story&STORY=/www/story/07−07−2004/0002205858&EDATE=WED+Jul+0 7+2004,+09:02+AM

18. *July 07, Reuters* — **Two Louisiana ports ordered shut over security. The U.S. Coast Guard has ordered the closure of two facilities in Louisiana that handle natural gas liquids (NGL) and petroleum products for failure to comply with new maritime security codes, the Coast Guard said on Wednesday, July 7**. An NGL fractionation plant operated by Enterprise Products Partners LP and a products terminal operated by El Paso Corporation, both located in Geismar, LA, were closed for their non−compliance with the new stringent port security laws, the Coast Guard's Lt. Aaron Demo said. Enterprise Products Partners company spokesperson, Randy Burkhalter, estimated it would take about two weeks to bring the fractionation plant into compliance. The facilities are jointly operated by the two companies. The tough new security regulations for ships went into effect on July 1, and so far there has been no significant disruption to energy supplies as a result.
Source: http://biz.yahoo.com/rc/040707/energy_security_ports_1.html

[Return to top]

Postal and Shipping Sector

19. *July 06, Indianapolis Star* — **Pipe bomb discovered in mailbox.** Nancy Strange didn't think much of the odd object in her mailbox when she first saw it. It wasn't until mid–afternoon, as Strange was returning to her home in Avon, IN, that she learned anything was amiss. It turns out the object was an apparent pipe bomb. A mail carrier thought the object was suspicious and immediately called authorities, Avon Assistant Police Chief Rob Paris. Officers from the Indianapolis Police bomb squad unit were called in to disarm the device. **It was the third explosive device discovered in Hendricks County since Saturday, July 3, said Captain Brett Clark, spokesperson for the sheriff department.** He said a mailbox on in the Ashford Estates subdivision was blown up Saturday. On Sunday, July 4, a mailbox in the North Salem area was damaged when some type of fireworks exploded in it, Clark said. Bureau of Alcohol Tobacco and Firearms agents gathering evidence at the scene on Wednesday were expected to compare remnants of the two mailbox incidents to determine if there's any connection.
Source: http://www.indystar.com/articles/9/160412–4659–093.html

[Return to top]

Agriculture Sector

20. *July 07, Financial Times* — **U.S. puts tariffs on Chinese shrimp. The U.S. said on Tuesday, July 6, it would impose preliminary tariffs on more than one billion dollars of shrimp imports from China and Vietnam, hitting several Chinese producers with hefty new duties while levying more modest penalties against Vietnam.** The initial outcome in one of the largest anti–dumping cases filed is a partial victory for U.S. shrimp fishermen who allege that the growth in imports –– which now comprise more than 85 percent of the U.S. market –– had made their catches unprofitable. The Southern Shrimp Alliance, representing about 13,000 U.S. shrimp fishermen from eight states, had asked for tariffs of between 133 percent and 263 percent to be levied against Chinese shrimp, and from 26 percent to 93 percent against Vietnam. U.S. shrimp imports last year were valued at more than $3.5 billionn, of which nearly two–thirds could be hit with new tariffs. **The commerce department is to rule this month on shrimp imports from Thailand, which account for one quarter of U.S. imports, as well as Brazil, Ecuador, and India.**
Source: http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1087373532249&p=1012571727162

21. *July 07, Associated Press* — **Brucellosis testing costs. Wyoming's farm and ranch industry could lose about 100 jobs and nearly four million dollars as a result of mandatory brucellosis testing, according to a state report.** The finding of the disease in two cattle herds in the state last winter resulted in loss of federal brucellosis–free status and testing of hundreds of thousands of cattle. **Lost livestock sales revenue over the next year is estimated to range from $495,000 to $3,795,000, according to a report by the Wyoming Economic Analysis Division.** Producers may lose sales to other states and foreign countries that do not want to risk buying Wyoming cattle because it may jeopardize their own brucellosis status, said Amy Bittner, a state economist. In addition, producers can expect to pay $1.50 to $11.50 per head for testing, she said. "The employment impacts from low–cost testing could result in 11 jobs initially lost in the farm sector," she wrote. "Additionally, if a higher testing cost was instituted, then 87 farm jobs could be eliminated due to the decrease in livestock sales. Secondary

employment effects may also include reductions in private non−farm employment such as in the retail and services sectors."
Source: http://www.thefencepost.com/article.php?sid=1223&rs=2

22. *July 07, University of Illinois at Urbana−Champaign* — **Robotic agriculture.** University of Illinois agricultural engineers have developed several agriculture robots. The robots are completely autonomous, directing themselves down corn rows, turning at the end and then moving down the next row, said Tony Grift, an agricultural engineer at the University of Illinois at Urbana−Champaign. **The long−term goal, he said, is for these small, inexpensive robots to take on some of the duties now performed by large, expensive farm equipment.** Robots have been a part of industrial environments for decades now, but Grift said the time may be right for robots to adapt to the more rugged environment outdoors. Grift would like to someday see an experimental farm where all of the work is being performed by autonomous robots. Right now, they're focusing on navigation skills for the robots. **Eventually, these robots could be equipped to perform duties, such as detecting disease, weeds or insects, sampling soil or even applying pesticides.**
Source: http://www.innovations−report.de/html/berichte/agrar_forstwi ssenschaften/bericht−30963.html

23. *July 07, U.S. Newswire* — **Plant pathologists look to forensics to aid in biosecurity. In an effort to protect the nation's crops from possible bioterrorism, plant pathologists are exploring how to apply techniques typically used in crime labs as a tool to fight bioterrorism.** According to Jacqueline Fletcher, plant pathology professor, Oklahoma State University, the potential for microbes to be used with an intent to harm people, societies, or the environment has generated renewed interest in the application of forensic science to assist in precise identification of microbes and their origin. **"If a plant disease agent were used for bioterrorism, we would like to trace it to its source. This could help us prevent it from happening again," said Fletcher.** The usual goal of a plant pathologist, which is to effectively manage a disease outbreak, requires identification of a disease agent that is accurate to species or strain. Species level identification is important in order to understand the disease's epidemiology. Forensic applications, however, require an even higher level of detail and discrimination. "If the goal is to attribute the crime to a specific perpetrator, data must be sufficiently specific to stand up in a court of law," said Fletcher. New research is needed to expand knowledge on the genetics, evolution, biology, and host reactions of key microbes.
Source: http://releases.usnewswire.com/GetRelease.asp?id=109−0707200 4

[Return to top]

Food Sector

24. *July 06, Associated Press* — **University aims to thwart terrorist threats to food supply.** While much of the nation's anti−terrorism effort focuses on government buildings and skyscrapers, Frank Busta worries about the plate on the dining room table. The University of Minnesota professor emeritus of food science and nutrition will run the University's new Center for Food Protection and Defense. It was to be officially launched on Tuesday, July 6, with a campus visit by Department of Homeland Security Secretary Tom Ridge and Agriculture Secretary Ann Veneman. The three−year, $15 million grant to fund the center was announced

in April. Schools that are major partners in the Minnesota grant are the University of Wisconsin–Madison, Michigan State University, and North Dakota State University. Individual faculty members at institutions such as Harvard and the University of Maryland are involved. **Ridge and Veneman will see a small demonstration of the wide range of work that will be done, from using molecular biology and technology to detect incredibly small amounts of dangerous substances in food to figuring out who has access to that salmon or steak before it reaches the grill.**
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/politi cs/9090254.htm

[Return to top]

Water Sector

25. *July 05, Associated Press* — **Cleaning up drinking water costly. A survey of dozens of utilities shows the cost to meet newly enforced drinking water standards in Wisconsin is $200 million and climbing.** Years ago, the Environmental Protection Agency set a limit of five picocuries of radium per liter of water, because the federal government has linked the mineral to cancer. But the state's enforcement of the standard has just started recently. In December, 42 utilities and the state Department of Natural Resources entered into a consent decree, meaning utility officials formally acknowledged their water systems did not comply with federal safe water standards for levels of radium and other contaminants. Utilities have until December 2006 to comply.
Source: http://www.greenbaypressgazette.com/news/archive/local_16782 917.shtml

[Return to top]

Public Health Sector

26. *July 07, Associated Press* — **Interpol launches training program to prevent bioterrorism. Interpol, the international police agency based in France, says it's launching a two–year program to train police and experts from around the world to fight bioterrorism.** The agency says it will fund the program with a $943 thousand grant from the Alfred P. Sloan Foundation. Some of the money will finance a conference next year for top law enforcement agents and other experts. Interpol says regional training sessions will also take place in Africa, Asia, and the Americas. The funding will also go toward technical support and training materials and allow Interpol to single out gaps in bioterrorism legislation.
Source: http://www.kfor.com/Global/story.asp?S=2004440

27. *July 07, AScribe Newswire* — **Long working hours for nurses lead to medical errors. Medical errors and near errors are more likely to occur in hospitals when staff nurses routinely work long and unpredictable hours, an increasingly common practice throughout the U.S. as hospitals cope with a shortage of registered nurses,** according to a new study in the July issue of the journal Health Affairs. The link between errors and sleep–deprived resident physicians has been well documented. This study, by researchers at the University of Pennsylvania School of Nursing, is one of the first national attempts to quantify hospital nurses' working conditions and the effect on patient safety. **Researchers found that**

the risk of making an error greatly increased when nurses had to work shifts that were longer than 12 hours, when they worked significant overtime, or when they worked more than 40 hours per week. Researchers examined detailed logbooks from 393 registered nurses around the country who worked full–time in hospitals. The likelihood of making an error was three times higher when nurses worked shifts lasting at least 12.5 hours. Working overtime increased the odds of making at least one error, regardless of how long the shift was originally scheduled.
Source: http://www.ascribe.org/cgi–bin/spew4th.pl?ascribeid=20040707 .082405&time=08%2045%20PDT&year=2004&public=1

28. *July 06, IRIN News* — **Anthrax and hemorrhagic fever cases confirmed in Kazakhstan. Seven people in the north of the country have been hospitalized with anthrax contracted from infected cattle, while in the south three cases of Crimean–Congo hemorrhagic fever have been confirmed.** "The situation is that seven people have been hospitalized with confirmed anthrax," Albert Askarov, deputy head of the sanitary and epidemiological control committee, told IRIN. The hospitalized patients took part in slaughtering a calf that had died of a mysterious disease, with some of them reportedly selling the meat. "The calf had blood running out of its nose and they slaughtered it without notifying the veterinary service and getting a sanitary certificate," Askarov explained. Askarov cited a lack of veterinary control as the root cause of the problem. He also stressed the importance of tighter measures to prevent people from slaughtering infected animals. Meanwhile, three cases of Crimean–Congo hemorrhagic fever (CCHF) have been officially registered in the south over the past week. Every year dozens of cases are registered there. This year only three cases have been officially registered in these three provinces.
Source: http://www.irinnews.org/report.asp?ReportID=42024&SelectRegi on=Central_Asia&SelectCountry=CENTRAL_ASIA

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

29. *July 07, Associated Press* — **Utah bridges emergency communication gaps.** Officials have completed part of a plan that will allow police, firefighters and other first–responders to communicate during emergencies anywhere in the state. Governor Olene Walker announced Tuesday, July 6, that the Utah Wireless Integrated Network was successfully tested last month and implemented at the beginning of July. **It works by using computer software in dispatch and emergency control centers to connect the roughly 200 radio frequencies authorities use. That means someone at the northernmost tip of Utah could talk in minutes on a different radio frequency with another law enforcement officer camped on the Nevada state line.** The state used a $4 million federal grant to fund the first phase of the project. The second phase, set for completion by 2005, will allow authorities to share data on a powerful

wireless network.
Source: http://166.70.44.66/2004/Jul/07072004/utah/181605.asp

30. *July 07, Picayune Item (MS)* — **Emergency response agencies have unscheduled emergency test crash.** An afternoon page on the scanners sent many people into emergency mode in Picayune, MS, Tuesday, July 6. **The page "Plane crash at the Picayune airport –– multiple injuries" was just a test, but most emergency personnel and citizens didn't know about that mock disaster.** Emergency personnel said that was the plan. Dispatch requested emergency medical techs, fire fighters, police, sheriff's deputies, and other disaster personnel to respond to a huge fire and several so–called victims. "It's a mock disaster," Picayune Fire Chief Keith Brown said. "You get the hospital taxed, you get us out here, you get the police department, you get everybody involved." Police set up roadblocks, emergency management set up a command center, and personnel started doing their jobs. Once the victims were rescued, ambulances transported them to Crosby Memorial Hospital. Several people on the scene at the crash site and at the hospital said the drill was a success in many ways. Some said they learned that local emergency crews could handle a weapons–of–mass–destruction attack or some other major disaster.
Source: http://www.picayuneitem.com/articles/2004/07/07/news/02mock. txt

[Return to top]

Information Technology and Telecommunications Sector

31. *July 07, Reuters* — **World software piracy losses double in 2003. Software manufacturers lost $29 billion to piracy in 2003, more than double the previous year's losses, and about 36 percent of software installations worldwide are pirated copies, an industry survey showed on Wednesday, July 7.** In dollar terms, the losses were greatest in Western Europe, where piracy cut revenues by $9.6 billion in 2003, followed by Asia and North America, the study by the Business Software Alliance (BSA) and International Data Corp (IDC) showed. The BSA, a trade body, blamed the rapid spread of piracy on so–called peer–to–peer networks, in which Internet users illegally swap software and other files such as music for free or at discounted prices. Vietnam and China had the world's highest piracy rates, accounting for 92 percent of all computer software installed in each country, followed by the Ukraine with 91 percent, Indonesia at 88 percent, and Zimbabwe and Russia with 87 percent each. By region, about 53 percent of software on computers in Asia was pirated in 2003, compared with 70 percent in Eastern Europe, 63 percent in Latin America, 55 percent in the Middle East, 36 percent in Western Europe, and 23 percent in North America.
Source: http://www.reuters.co.uk/newsArticle.jhtml?type=technologyNews&storyID=5607026&section=news

32. *July 07, Reuters* — **Nanotech device shown, may shrink future chips. Scientists unveiled one of the smallest functioning devices ever made on Wednesday, July 7, a carbon tube about 10 atoms wide that could one day shrink computer chip technology.** Researchers at a technology company in Niskayuna, NY, hope that their new device, which is a rolled–up sheet of carbon atoms resembling chicken wire, will someday operate as the standard semiconductor in computers and other electronics. The device –– a nanotube –– is part of a developing field of technology in which devices are designed on the scale of a "nano," or a billionth of a meter.

That translates to about the size of 10 hydrogen atoms, or 1/80,000 the diameter of a human hair. Semiconductors are the core of electronic equipment, acting as valves for electrons to pass through and which run everything from cell phones to lap tops. **Scientists say silicon chips will reach their minimum size in the next decade. After that, they will be unable to get smaller without losing their ability to function.**
Source: http://www.reuters.com/newsArticle.jhtml?type=technologyNews &storyID=5603184

33. *July 07, United Press International* — **Emerson buys unit of Marconi. Emerson of St. Louis, MO, said Wednesday, July 7, it acquired the outside plant and power systems business of Marconi of Lorain, OH, for $375 million in cash.** The transaction is expected to close by the end of Emerson's fourth fiscal quarter, which is September 30, following regulatory review, and is expected to be accretive to fiscal 2005 earnings. **The Marconi power business is a leading provider of DC power products, engineering and installation services, and outside plant products to major telecommunication carriers throughout North America.** Its revenues for the year ended March 31, 2004, were approximately $380 million. Emerson said the deal will allow it to strengthen its presence with the regional Bell companies, inter–exchange carriers, wireless and cable companies in North America.
Source: http://washingtontimes.com/upi–breaking/20040707–111319–8902 r.htm

34. *July 06, PC World* — **Microsoft patch leaves holes open. Microsoft's effort last week to fix a vulnerability in the Internet Explorer Web browser and end the latest series of Internet attacks doesn't address another closely related and dangerous vulnerability, according to a security specialist.** Dutch security expert Jelmer Kuperus published code on the Web last week that he says can be used to break into fully patched Windows systems using a slightly modified version of an attack called Download.Ject that Microsoft patched last week. The new attack targets a hole in a different Windows component than the one addressed by Microsoft's software patch. Using a similar attack, malicious hackers could break into even patched Windows machines, Kuperus says. Microsoft confirms that the company is aware of the exploit code, but does not believe any customers have been attacked using the Shell.Application exploit, a spokesperson says.
Source: http://www.pcworld.com/news/article/0,aid,116796,00.asp

Internet Alert Dashboard

DHS/US–CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

Watch Synopsis: Keylogger trojans such as Download.JECT, Scob and Berbew have garnered national attention by both the media and incident response teams. Microsoft has released an out–of–band fix for Internet Explorer to prevent future exploits of client machines using the ADODB vulnerability. See Microsoft's security bulletin here: http://www.microsoft.com/security/incident/download_ject.msp x

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 9898 (dabber), 5554 (sasser−ftp), 1434 (ms−sql−m), 137 (netbios−ns), 1433 (ms−sql−s), 3127 (mydoom), 1026 (nterm), 1027 (icq)
	Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

35. *July 07, Associated Press* — **Wildfires threaten Arizona observatory. Although fire officials were hopeful they could save a $200 million mountaintop observatory, two small communities remained at risk Wednesday, July 7, in the path of a pair of lightning−sparked wildfires.** Fire crews got an improved weather forecast Wednesday, with temperatures expected to be slightly lower, said Julian Rhinehart, a spokesperson for the fire crews. One fire was less than a mile from the observatory and about 1 1/2 miles from Turkey Flat, a community of about 74 cabins where firefighters focused much of their efforts. Scientists feared that the fires could devastate the only population of Mount Graham red squirrels, an endangered species already imperiled by insect outbreaks attacking the forests, habitat loss and long−term drought. At Turkey Flat, fire crews wrapped sheets of aluminum around cabins to deflect heat and drenched them with water. **The observatory's protection, including a sprinkler system, had been reinforced by strengthened protection lines and prescribed burns.** Home to some of the world's most powerful telescopes, the observatory encompasses eight buildings and 8 1/2 acres of pine forest on Mount Graham's 10,470−foot Emerald Peak. Although its metal structures should withstand the flames, officials said smoke and heat could damage delicate instruments.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=519&ncid=718 &e=3&u=/ap/20040707/ap_on_re_us/wildfires

[Return to top]

General Sector

36. *July 07, Associated Press* — **Six Yemenis charged in USS Cole bombing. A Yemeni security court on Wednesday, July 7, charged six Yemenis in the planning of the October, 2000 bombing of the USS Cole and said they belonged to Osama bin Laden's terrorist network.** Seventeen American sailors were killed when two suicide bombers in an explosives−laden boat rammed the USS Cole as it refueled in the southern port city of Aden. The bombing was blamed on bin Laden's al Qaeda network. Among the six charged Wednesday was accused mastermind Abd al−Rahim al−Nashiri, who is in U.S. custody. The other five were in court. Al−Nashiri was accused of planning and funding the attack and training the cell members who carried it out. **U.S. officials believe the Saudi−born al−Nashiri is a close associate of bin Laden. In addition to the Cole attack, he is suspected of helping direct the 1998 bombings of U.S. Embassies in Kenya and Tanzania.** Judge Najib al−Qaderi read a list of charges that

included forming an armed gang to carry out criminal acts against the interests of the state; belonging to al Qaeda; resisting authorities and forging documents.
Source: http://abcnews.go.com/wire/World/ap20040707_174.html

37. *July 07, Bay City News (CA)* — **Explosives reportedly stolen. Approximately 200 pounds of high explosives have reportedly been stolen from a storage facility in San Mateo, CA. The theft was discovered over the holiday weekend, according to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).** According to bureau spokesperson Marti McKee, a number of agencies share use of the storage facility, including the Federal Bureau of Investigation, the San Francisco Police Department, and the San Mateo County sheriff's office. All of the agencies are participating in the ATF investigation to try and locate the stolen explosives, McKee said. In general, McKee said, high explosives like dynamite require detonation, whereas lower explosives like pipe bombs typically go off after being ignited.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/gate/a/2004/07/07/w eapons07.DTL

38. *July 06, Washington Post* — **Security intensifies for political conventions. Convinced that terrorists are determined to disrupt the presidential election by attacking the United States, the government is mounting a massive homeland security effort as the run−up to the two presidential nominating conventions begins.** Unprecedented security arrangements have been made for the conventions in Boston, MA, and New York, NY, where authorities believe al Qaeda may see an opportunity to disrupt and perhaps alter the outcome of the November 2 election. The effort stems from intelligence officials' conclusion that al Qaeda and like−minded groups, buoyed by the March 11 Madrid train bombings and the electoral defeat of Spain's government days later, are determined to launch something similar in this country. They base their conclusion on what they call incontrovertible classified intelligence that apparently includes electronic surveillance. **At the same time, government officials fear that terrorists may avoid that security buildup and strike "soft" targets such as hotels or department stores −− across town or across the country −− as the conventions are underway. The conventions have been designated National Special Security Events, which gives the U.S. Secret Service the lead in coordinating security.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A29636−2004Jul 5.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.